

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平7-161172

(43) 公開日 平成7年(1995)6月23日

(51) Int.Cl.<sup>6</sup>

G 1 1 B 23/28  
23/30

識別記号

庁内整理番号

Z 7177-5D  
B 7177-5D  
Z 7177-5D

F I

技術表示箇所

審査請求 未請求 請求項の数4 O L (全 10 頁)

(21) 出願番号

特願平5-304214

(22) 出願日

平成5年(1993)12月3日

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 井村 滋

東京都品川区北品川6丁目7番35号 ソニー株式会社内

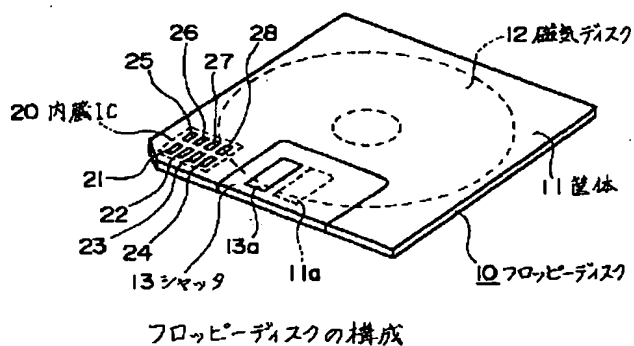
(74) 代理人 弁理士 松隈 秀盛

(54) 【発明の名称】 データ記録媒体

(57) 【要約】

【目的】 各種データをディスク、テープ等の記録媒体に記録させる場合に、セキュリティ性が高く且つ使い勝手の良い記録ができるようにする。

【構成】 データが記録される記録媒体12を筐体11に収納させ、この筐体11の所定箇所にIC20を取付けてなるデータ記録媒体において、記録媒体12に起動プログラムと暗号化されたデータとを記録させ、記録データの暗号化プログラムと暗証番号のデータとをIC20内のメモリに記憶させ、記録されたデータを読み出す場合又は記録媒体12にデータを書込む場合に、入力された暗証番号をIC20に供給させて、このIC20内のメモリに記憶された暗証番号と演算手段が照合させ、暗証番号が一致した場合には、IC20内のメモリに記憶された暗号化プログラムに従って、記録媒体12に記録された暗号化されたデータの復号又は記録媒体12に記録するデータの暗号化をできるようにした。



**【特許請求の範囲】**

**【請求項 1】** 所定の方法でデータが記録される記録媒体を所定の筐体に収納させ、該筐体の所定箇所にメモリと演算手段とを有する IC を取付けてなるデータ記録媒体において、

上記記録媒体に起動プログラムと暗号化されたデータとを記録させ、上記暗号化されたデータの暗号化プログラムと暗証番号のデータとを上記 IC 内のメモリに記憶させ、

上記記録媒体に記録されたデータを読み出す場合又は上記記録媒体にデータを書込む場合に、入力された暗証番号を上記 IC に供給させて、この IC 内のメモリに記憶された暗証番号と演算手段が照合させ、暗証番号が一致した場合には、IC 内のメモリに記憶された暗号化プログラムに従って、上記記録媒体に記録された暗号化されたデータの復号又は上記記録媒体に記録するデータの暗号化をできるようにしたデータ記録媒体。

**【請求項 2】** IC 内での暗証番号の照合で、予め定めた所定回連続して不一致を検出したとき、以後の照合で暗証番号が一致しても暗号化プログラムを出力させないブロックを行うようにした請求項 1 記載のデータ記録媒体。

**【請求項 3】** 予め定めた所定回連続して不一致を検出してブロックされた状態で、上記暗証番号とは別に設定された暗証番号を入力させることで、ブロックの解除を行うようにした請求項 2 記載のデータ記録媒体。

**【請求項 4】** IC 内のメモリに付加情報を記憶させるようにした請求項 1 記載のデータ記録媒体。

**【発明の詳細な説明】****【0001】**

**【産業上の利用分野】** 本発明は、フロッピーディスク等の磁気ディスク、光磁気ディスク、光ディスク、磁気テープなどの各種記録媒体に適用されるデータ記録媒体に関する。

**【0002】**

**【従来の技術】** コンピュータプログラムなどを記録する記録媒体として、フロッピーディスク等と称される磁気ディスクが広く使用されている。また、磁気ディスクよりも記録密度の高い媒体として、レーザビームを記録や再生に使用する光磁気ディスクや光ディスクも使用されている。

**【0003】** これらのディスクにプログラムを記録させる場合には、例えば各ディスクのデータ記録トラックに設定されたセクタに、このディスクの記録フォーマットに従った順序でデータを記録し、再生するときには記録フォーマットに従ったセクタ順に記録データを再生させて、記録されたプログラムを得るようにしている。

**【0004】** これに対し、ディスクに記録されたデータのセキュリティ性を高めるために、通常フォーマットに従ったセクタ順にデータを記録させるのではなく、適

当なオフセット等をセクタに付加して記録することが行われている。このようにしてディスクに記録されたデータを読み出す場合には、セクタを変更させたオフセットデータ等が読み出すコンピュータ側に用意されてないと、正しいプログラムを得ることができず、プログラムの不正使用を防止することができる。

**【0005】**

**【発明が解決しようとする課題】** ところが、このようにセクタの順序を変更させた場合でも、ディスク 1 枚に記録されたデータを全てそのまま別のディスクに複製するコピー装置で複製することは可能である。従って、このようなコピー装置でオリジナルのディスクから複製を行い、複製されたディスクを使用するコンピュータ側に、データの正確な読み出しに必要なセクタのオフセットデータ等が用意されていれば、プログラムを複製して不正使用することが可能である。従って、このような記録方法は、プログラムの不正使用防止の観点からは不完全な記録方法である。

**【0006】** 一方、記録するプログラムデータそのものを、所定の暗号方式に基づいて暗号化し、暗号化されたデータをディスクに記録する方法もある。この場合には、このプログラムデータを解読する暗号化プログラムが必要で、暗号化プログラムが記録されたディスクなどを別に用意する必要があるが、この暗号化プログラムが記録されたディスクなどの管理が煩わしく、このディスクを紛失した場合にはプログラムデータの復号ができなくなってしまう。このような紛失による復号不可とならないようにするためには、暗号化プログラムが記録されたディスクをコピーしておくことが考えられるが、暗号化プログラムがコピーされると、それだけセキュリティ性が低くなり、暗号化した意味がなくなってしまう。

**【0007】** また、このように暗号化する場合に、或るキーワードを使用してスクランブルを掛ける方法もあるが、このような場合には暗号化する側と復号化する側とで同一のキーワードを知っている必要があり、何回も同じキーワードを使用すると、キーワードが知れ渡って暗号化の意味がなくなってしまう。従って、使い捨てキーワード方式と称する使用するキーワードを逐次変更する方法もあるが、キーワードの管理が煩雑になってしまう。

**【0008】** ここまでの説明では、ディスクにコンピュータプログラムデータを記録させる場合について説明したが、磁気テープなどの他の記録媒体にデータを記録させる場合にも、セキュリティ性についての同様な問題点がある。

**【0009】** 本発明の目的は、プログラムなどの各種データをディスク、テープ等の記録媒体に記録させる場合に、セキュリティ性が高く且つ使い勝手の良い記録ができるようにすることにある。

**【0010】**

【課題を解決するための手段】本発明は、例えば図1に示すように、所定の方法でデータが記録される記録媒体12を所定の筐体11に収納させ、この筐体11の所定箇所メモリと演算手段とを有するIC20を取付けてなるデータ記録媒体において、記録媒体12に起動プログラムと暗号化されたデータとを記録させ、暗号化されたデータの暗号化プログラムと暗証番号のデータとをIC20内のメモリに記憶させ、記録媒体12に記録されたデータを読み出す場合又は記録媒体12にデータを書込む場合に、入力された暗証番号をIC20に供給させて、このIC20内のメモリに記憶された暗証番号と演算手段が照合させ、暗証番号が一致した場合には、IC20内のメモリに記憶された暗号化プログラムに従って、記録媒体12に記録された暗号化されたデータの復号又は記録媒体12に記録するデータの暗号化をできるようにしたものである。

【0011】またこの場合に、IC内での暗証番号の照合で、予め定めた所定回連続して不一致を検出したとき、以後の照合で暗証番号が一致しても暗号化プログラムを出力させないブロックを行うようにしたものである。

【0012】さらに、このブロックされた状態で、上記暗証番号とは別に設定された暗証番号を入力させることで、ブロックの解除を行うようにしたものである。

【0013】また、上述した場合に、IC内のメモリに付加情報を記憶させるようにしたものである。

【0014】

【作用】本発明によれば、記録媒体に記録されたデータの暗号化プログラムが、この記録媒体を収納する筐体に取付けられたICに記憶され、暗証番号が一致しない限りこのICから暗号化プログラムを読み出すことができなく、従って記録媒体に記録されたデータの復号もできなく、記録されたデータの不正使用を防止するセキュリティ性が高い。

【0015】この場合、IC内での暗証番号の照合で、予め定めた所定回連続して不一致を検出したとき、以後の照合で暗証番号が一致しても暗号化プログラムを出力させないブロックを行うことで、不正な使用を防止する効果がより高くなる。

【0016】また、このブロックされた状態で、暗号化プログラム読み出し用の暗証番号とは別に設定された暗証番号を入力させることで、ブロックの解除を行うようにしたことで、ブロックされた状態の解除が良好にできる。

【0017】さらに、IC内のメモリに付加情報を記憶させることで、暗号化プログラムが記憶されたICが効率よく使用される。

【0018】

【実施例】以下、本発明の実施例を、添付図面を参照して説明する。

【0019】本例においては、フロッピーディスクと称される磁気ディスクを使用したコンピュータ用のデータ記録媒体に適用したもので、図1～図3に示すように構成する。図1は本例のフロッピーディスクの全体構成を示す図で、図中10はフロッピーディスク全体を示し、このフロッピーディスク10は、合成樹脂で形成された筐体11の中に、直径3.5インチの磁気ディスク12が収納され、開閉自在なシャッター13が取付けてある。このシャッター13には窓部13aが設けられ、シャッター13が開状態のとき、筐体11側の開口部11aと窓部13aとの位置が一致して、磁気ディスク12の信号記録面が露出する。

【0020】そして、このフロッピーディスク10を後述する駆動装置に装着させたとき、磁気ディスク12が所定の駆動手段により回転すると共に、シャッター13が開状態になって露出した信号記録面に磁気ヘッドが近接し、このヘッドでデータの記録や再生ができる。なお、この信号記録面は、片面だけの場合と、両面に形成された場合とがある。ここまでは、通常のフロッピーディスクの構成である。

【0021】そして本例においては、このフロッピーディスク10の筐体11の隅に、1チップのIC（集積回路）20が内蔵させてある。このIC20は、筐体11の表面から見ると、図2に拡大して示すように、8個の接点21、22、23、……28が露出ただけとしてあり、内部の回路は図3に断面で示すように筐体11を構成する樹脂内に埋め込まれている。なお、IC20の内部の構成は後述する。

【0022】次に、このように構成されるフロッピーディスク10の駆動装置の構成を説明する。図4及び図5は、この駆動装置の構成を示す図で、図中30はフロッピーディスク駆動装置全体を示し、このフロッピーディスク駆動装置30は、フロッピーディスク10を装着するための窓部31を有し、この窓部31から内部に装着されたフロッピーディスク10は、図5に断面で示すように、所定のチャッキング機構33によりモータ32側と接続され、モータ32により所定速度に回転駆動される。そして、図示しない磁気ヘッドにより、記録や再生が行われ、後述するホストコンピュータ側から供給される記録データが磁気ディスク12に記録されると共に、磁気ディスク12より再生したデータがホストコンピュータ側に供給される。

【0023】そして、フロッピーディスク10の表面に露出した8個の接点21～28と接続するために、端子ユニット40が設けられ、この端子ユニット40に配された8個の接片41、42、43、……48の先端が、それぞれ対応した接点21～28と接触するようにしてある。そして、各接片41～48は、ホストコンピュータ側の所定のインターフェースと接続させてあり、ホストコンピュータ側の制御で、記憶データの読み出しなどの

処理ができるようにしてある。

【0024】次に、本例のフロッピーディスク10に内蔵されたIC20の構成を説明すると、図6に示すように、ここでは8個の接点21～28の内の6個の接点21～26が使用され、接点21が電源端子VCCとされ、接点22が内蔵されたEEPROM55のプログラム電圧入力端子VPPとされ、接点23がシリアルデータ入出力端子I/Oとされ、接点24がクロック入力端子CLKとされ、接点25がリセット信号入力端子RSTとされ、接点26が接地端子GNDとされる。

【0025】そして、IC20の内部の回路として、演算処理を行う中央制御装置(CPU)51と、IC20内と外部との間でデータ入出力を行うためのシリアル/パラレル変換回路52と、このシリアル/パラレル変換回路52に変換用クロックを供給するための分周器53と、データを一時的に記憶するRAM54と、暗証番号などの保存及び書き換えが必要なデータを記憶するEEPROM55と、暗号化プログラムなどのプログラムを記憶するROM56とで構成され、中央制御装置51とシリアル/パラレル変換回路52と各メモリ54、55、56との間はバスラインで接続されている。

【0026】そして、中央制御装置51と分周器53には、接点24(クロック入力端子CLK)に得られるクロックが供給され、このクロックに基づいて中央制御装置51が作動する。この場合、接点25(リセットパルス入力端子RST)に所定のリセット信号が供給されることで、中央制御装置51が起動される。また、分周器53でクロックを分周した信号をシリアル/パラレル変換回路52に供給し、この分周信号に基づいてシリアルデータからパラレルデータへの変換又はパラレルデータからシリアルデータへの変換を行う。そして、シリアル/パラレル変換回路52には、外部との入出力端子としての接点23(シリアルデータ入出力端子I/O)が接続され、外部から接点23を介して供給されるシリアルデータをパラレルデータに変換し、バスラインを介して中央制御装置51などに供給する。また、バスラインを介してシリアル/パラレル変換回路52に供給されるパラレルデータを、シリアルデータに変換して、接点23から外部のコンピュータ(ホストコンピュータ)側に供給する。

【0027】また、このIC20のEEPROM55に記憶されるデータは、外部から接点22(プログラム電圧入力端子VPP)に所定のプログラム電圧が供給されることで、書き換えが可能とされている。

【0028】次に、このIC20が内蔵されたフロッピーディスク10とアクセスされるホストコンピュータ側の構成を説明する。図7は、このホストコンピュータの構成を示す図で、図中61はメインの中央制御装置(CPU)を示し、この中央制御装置61には、バスラインを介してフロッピーディスクインターフェース62、ハ

ードディスクユニット63、RAM64、ROM65、キーボードインターフェース66、CRTインターフェース68、シリアル/パラレル変換回路69が接続されている。そして、フロッピーディスクインターフェース62は、上述したフロッピーディスク駆動装置30に装着されたフロッピーディスク10の磁気ディスク12側の記録データと中央制御装置61側とのインターフェースが行われると共に、フロッピーディスク10に内蔵されたIC20と中央制御装置61側とのインターフェースが行われる。

【0029】また、キーボードインターフェース66には、キーボード67が接続させてあり、キーボード67の操作情報がインターフェース66を介して中央制御装置61側に伝送される。また、CRTインターフェース68には、CRTディスプレイ装置70が接続され、バスラインを介して供給される表示データがCRTディスプレイ装置70側に供給されて、対応した文字や画像が表示される。さらに、シリアル/パラレル変換回路69を介して接続された外部機器(プリンタ等の周辺機器:図示せず)に、データを伝送することができるようにしてある。

【0030】そして、このように構成されたホストコンピュータと、フロッピーディスク10内のIC20との間では、図9に示すような処理で通信が行われ、IC20を使用したデータ処理が行われる。即ち、最初にホストコンピュータ側から電源VCCとプログラム電圧VPPとして所定の電位の信号を供給すると共に、所定の周波数のクロックCLKを供給して、IC20が作動できる状態を設定する(ステップ201)。また、この最初の状態ではローレベル“L”のリセット信号を供給し、IC20内の中央制御装置51をリセットされた状態にする。

【0031】そして、リセットパルスRSTをハイレベル“H”に変化させてリセットを解除し、IC20を起動させる(ステップ202)。ここで、IC20が起動したときには、IC20内の中央制御装置51からホストコンピュータ側に、応答信号としてデータ交換に必要な初期データが転送される(ステップ203)。この初期データには、IC20が受け取るデータの論理レベルやファーストビットなどを決定する情報などが含まれている。

【0032】そして、ホストコンピュータの中央制御装置61側では、この初期データを受信すると、IC20とのインターフェースを対応した状態に設定し、以後のセッションを行う。次に、ホストコンピュータからは、コマンドをIC20内の中央制御装置51に伝送させる(ステップ204)。このコマンドは、例えば5バイトで構成され、命令体系の属性、命令、パラメータ等を示す。

【0033】そして、IC20の中央制御装置51で

は、伝送されたコマンドが、このIC Iに与えられた命令体系に属し、なお且つ命令やパラメータが正しいか否か判断し、判断した結果しての認証データをホストコンピュータに返送する(ステップ205)。また、コマンドが正常と判断する認証データを返送した場合には、続いてコマンドに対応したデータを転送させる(ステップ206)。このデータの転送方向は、コマンドにより設定される。なお、コマンドによってはデータの転送がない場合もある。

【0034】そして最後に、IC 20側の処理が終了したことを示すステータスをホストコンピュータ側に送信し(ステップ207)、このセッションを終了する。その後、ホストコンピュータは必要に応じてステップ204のコマンド送信からステップ207のステータス受信までを繰り返す。

【0035】そして、本例においてはこの場合に使用されるコマンドとして、2つの体系のコマンドが用意されている。即ち、第1のコマンドとして管理コマンドが用意され、利用者に知られることなく扱われるコマンドで、フロッピーディスク10の発行者と管理者だけに使用が許可されたコマンドである。

【0036】そして、第2のコマンドがIC 20とのインターフェースを制御するコマンドで、このコマンドを使用してフロッピーディスク10を使用する際のアクセスが行われる。

【0037】以上説明した構成にて本例のIC内蔵のフロッピーディスク10が使用されるが、以下この内蔵されたIC 20を使用する場合の処理の一例を、図8のフローチャートを参照して説明する。

【0038】ここでは、フロッピーディスク10内の磁気ディスク12に、コンピュータ用プログラムデータを暗号化して記録させ、IC 20内のROM 56に、その暗号化プログラムを記憶させておく。また、磁気ディスク12には、記録されたプログラムデータを読み出すのに必要な起動プログラムを記録させておく。この起動プログラムは暗号化させない。そして、IC 20から暗号化プログラムを読み出すための暗証番号(所定桁の数字による番号)を、IC 20に設定できるようにし、この設定された暗証番号のデータをIC 20内のEEPROM 55に保存させておく。また、この暗号化プログラム読出し用の暗証番号とは別に、後述するブロック解除用の暗証番号も設定してIC 20内のEEPROM 55に保存させておく。

【0039】そして、IC 20内に記憶された暗号化プログラムは、EEPROM 55に登録された暗証番号と同じ番号がホストコンピュータ側から供給された場合だけ、ホストコンピュータ側に読出せるようにしてある。また、登録された暗証番号とは異なる番号が入力された場合には、この誤った暗証番号の入力処理が3回連続して行われたとき、IC 20内の中央制御装置51の制御

で、このIC 20からの暗号化プログラムの読出しを禁止するブロック処理を行うようにしてある。このブロックされた状態では、正しい暗証番号が入力されても、暗号化プログラムの読出しを禁止する。

【0040】そして、このブロックされた状態で、EEPROM 55に登録されたブロック解除用の暗証番号と同じ番号がホストコンピュータ側から供給されたときには、ブロックを解除するようにしてある。但し、このブロック解除用の暗証番号の入力を10回連続して誤ったときには、IC 20内の中央制御装置51が、ブロック解除用の暗証番号の入力自体を受け付けないようにして、よりレベルの高いブロックが行われるようにしてある。このレベルの高いブロックが行われた状態では、このセキュリティシステムの管理者(フロッピーディスクの発行元)が、管理用のツールを使用して解除しない限り、IC 20とアクセスできる状態に復帰しないようにしてある。

【0041】また、磁気ディスク12に暗号化されて記録されたプログラムに関する暗号化する必要のない付加情報(簡単な目次、日付、利用者名などの任意の情報)を、IC 20内のメモリ(RAM 54など)に記憶できるようにしてある。

【0042】このように暗号化されてフロッピーディスク10内の磁気ディスク12に記録されたデータを再生(又は磁気ディスク12に暗号化してデータを記録)する場合の処理を、以下図8のフローチャートに従って順に説明する。まず、ホストコンピュータは磁気ディスク12に記録された起動プログラムを読み出して、ホストコンピュータ内に読み込ませる(ステップ101)。この動作は、従来のフロッピーディスクに記録されているプログラムの起動時の動作と同じである。

【0043】そしてこの起動後には、ホストコンピュータ側のCRTディスプレイ装置70に、暗証番号の入力要求があることを表示させる(ステップ102)。この表示の後、キーボード67で暗証番号の入力操作が行われると、この入力された番号のデータをフロッピーディスク10内のIC 20に転送させる(ステップ103)。そして、ホストコンピュータ側でIC 20からのステータスを受信すると(ステップ104)、このとき受信したデータでIC 20がブロックされているか否か判断する(ステップ105)。

【0044】このとき、ブロックされているときには、ホストコンピュータ側のCRTディスプレイ装置70に、ブロックされていることを表示させる(ステップ106)。また、ブロックされていない場合には、暗証番号が一致するか否かの認証結果の判断を行い(ステップ107)、暗証場合が一致した場合には、キーボード67の操作などでモード入力を行う(ステップ109)。このモード入力は、IC 20に記憶された付加情報の読出しを行うか、或いは暗号化プログラムの読出しを行う

かを選択するためのものである。

【0045】また、ステップ107で暗証番号が一致しなかった場合には、ホストコンピュータ側のCRTディスプレイ装置70に、暗証番号の再入力进行要求する表示をさせた後（ステップ109）、ステップ103に戻る。

【0046】そして、ステップ109でモード入力が行われた後は、ホストコンピュータ側の中央制御装置61が、入力されたモードが付加情報を確認するものであるのか否か判断する（ステップ110）。ここで、付加情報を確認するモードでない場合には、IC20内のROM56に記憶された暗号化プログラムを、ホストコンピュータ側のRAM64に転送させる処理を行う（ステップ111）。そして、このとき必要とする処理が、データをフロッピーディスクに記録させる処理（書込させる処理）であるのか否か判断し（ステップ112）、記録させる場合には、RAM64に転送された暗号化プログラムに基づいたホストコンピュータ側の処理で、記録するデータを暗号化されたデータとし、この暗号化されたデータを磁気ディスク12の所定セクタに記録させる（ステップ113）。また、このときに生じる付加情報（記録日時などのデータ）を、IC20に転送させて、付加情報を記憶するエリアに記憶させておく（ステップ114）。

【0047】そして、ステップ112で再生させる処理（読出させる処理）であると判断したときには、磁気ディスク12に記録された所定のデータを再生してホストコンピュータ側に転送させ、RAM64に転送された暗号化プログラムに基づいたホストコンピュータ側の処理で、再生されたデータの復号化を行い、この復号化されたデータを指定されたドライブ（ハードディスク又は他のフロッピーディスクなど）側に供給させて書込ませておく（ステップ115）。

【0048】そして、この記録や再生の処理が終了した後は、ホストコンピュータ側のRAM64が記憶している暗号化プログラムを消去させるバジ処理を行う（ステップ116）。この暗号化プログラムの消去処理が終了すると、このときに必要なIC20のセッションが終了したか否か判断し（ステップ117）、終了したときには、ホストコンピュータ側のDOS（ディスクオペレーティングシステム）を使用した処理に戻る（ステップ118）。

【0049】また、ステップ110で付加情報を確認するモードである場合には、IC20に記憶された付加情報をホストコンピュータ側に読込ませ（ステップ119）、この読込んだ付加情報をCRTディスプレイ装置70に表示させる（ステップ120）。そして、この表示を行うとステップ117に移る。

【0050】そして、ステップ117でIC20のセッションが終了してないと判断したときには、ステップ1

08に戻り、モード入力処理から再度実行させる。

【0051】ステップ106でブロックされていることを表示した後は、キーボード67でブロック解除用暗証番号の入力操作があるか否か判断し（ステップ121）、この入力操作がある場合には、この入力されたブロック解除用暗証番号のデータをIC20へ転送させる（ステップ122）。そして、ホストコンピュータ側でIC20からのステータスを受信すると（ステップ123）、ブロック解除用暗証番号が一致したか否かの認証処理を行い、一致したか否か判断する（ステップ124）。ここで、一致した場合には、ステップ108に移って、モード入力を受け付ける。また、一致しなかった場合には、IC20とのアクセスを終了して、ステップ118に移ってホストコンピュータ側のDOSを使用した処理に戻る。

【0052】以上のようにしてフロッピーディスク10を使用して、暗号化されたデータの記録・再生が行われることで、暗号化されて記録されたデータの不正使用を効果的に防止できる。即ち、暗号化する方法に関するプログラムは、フロッピーディスク10に内蔵されたIC20に記憶され、ディスクに記録や再生を行う場合で且つ暗証番号を知っている場合にだけ、この暗号化プログラムを讀出してデータの暗号化や復号化が出来るようになっている。このため、暗証番号を知らない限り、記録されたデータを復号して読出すことができなく、不正使用の防止効果が高いと共に、暗号化プログラムを讀出してコピーすることが困難で、暗号化プログラムが外部に漏れる可能性が少ない。

【0053】従って、例えば1枚のフロッピーディスクに記録されたデータを、そのまま全てコピーする装置を使用して複製しても、暗号化プログラム自体は複製されず、フロッピーディスクに記録されたプログラムデータが不正使用されることが防止される。

【0054】また本例の場合には、記録されたプログラムデータを読出すのに必要な起動プログラムを、暗号化せずに磁気ディスク12に記録するようにしたので、ホストコンピュータからの制御でこの起動プログラムを讀出すまでの動作は、従来のフロッピーディスクと同じであり、この起動プログラムに従って暗号化プログラムを讀出す処理が行われるようにすれば、ホストコンピュータ側では暗号化や復号化のために特別な制御プログラムを用意しておく必要がなく、従来のフロッピーディスクを使用する場合と同様なプログラム構成の制御で実現できる。

【0055】また、本例のように1枚のフロッピーディスクにIC20を内蔵させた場合には、ディスクと暗号化プログラムとが1対1で対応しているので、1枚のフロッピーディスク毎に暗号化プログラムを変えることができる。このように1枚のフロッピーディスク毎に暗号化プログラムを変えることで、例えば何れかの暗号化プロ

グラムが外部に漏れても、この暗号化プログラムに対応した特定のディスクのデータだけが解読できただけで、このシステムが適用されるディスクの記録データ全てが解読できるものではなく、不正使用防止効果がより高くなる。

【0056】また、本例の場合には、暗証番号の照合処理を複数回（上述実施例では3回）連続して誤って行ったとき、不正に暗号化プログラムを読出そうとしている可能性が高いとして、内蔵されたICからの暗号化プログラムの読出しをブロックするようにしたので、暗証番号を知らない者が何回も照合作業を行って暗証番号を解読する作業ができないようにしてあり、この点からも不正使用の防止効果が高い。

【0057】さらに、この内蔵されたICからの暗号化プログラムの読出しがブロックされた状態で、このブロック状態を解除することが別の暗証番号でできるようにしてあるので、万一ブロックされたときの対処が容易にできると共に、このブロック状態を解除するための暗証番号の照合作業でも、複数回（上述実施例では10回）連続して誤って行ったときには、内蔵されたICからの暗号化プログラムの読出しを完全にブロックするようにしたので、さらに不正使用の防止に対する効果が高い。

【0058】なお、上述実施例ではフロッピーディスクへの記録・再生を行う場合に、IC20からホストコンピュータ側に暗号化プログラムを転送させて、ホストコンピュータ内で暗号化や復号化の処理を行うようにしたが、IC20からの暗号化プログラムの読出しは出来ないようにして、代わりにディスクから再生したデータの復号化やディスクに記録するデータの暗号化を、IC20内の処理で行うようにしても良い。この場合には、暗号化プログラムが全く外部に転送されないので、ホストコンピュータ側で暗号化プログラムがコピーされる可能性が全くなく、セキュリティ性が非常に高い。但し、ディスクから再生したデータやディスクに記録するデータを、一旦IC20に転送させて処理させる必要があり、ホストコンピュータ側で処理する場合に比べて、データの再生や記録に若干時間がかかる。

【0059】また、上述実施例では暗号化方法については特に説明しなかったが、コンピュータ用データに適用できる各種暗号化方法が使用できる。例えば、フロッピーディスクの1セクタに相当するバイト数毎に暗号化する方法、1トラックに相当するバイト数毎に暗号化する方法、データやプログラムを一括して暗号化する方法などが考えられる。また、所定のセクタやトラック毎に暗号化する場合に、この暗号化する単位データ毎に暗号化アルゴリズムを変更するようにしても良い。また、1枚のフロッピーディスクに記録するデータの内の一部のデータだけを暗号化するようにしても良い。

【0060】また、上述実施例ではディスクに記録されるデータの付加情報をIC20に記憶させるようにした

が、この付加情報についても必要により暗号化して記憶させるようにしても良い。また、IC20に記憶させる代わりに、磁気ディスク12の所定のエリアに記録させるようにしても良い。

【0061】さらに、上述実施例においては磁気ディスクに適用したが、他の記録媒体にも適用できることは勿論である。例えば、光磁気ディスク、光ディスクなどのディスク状の記録媒体や、磁気テープ等のテープ状の記録媒体にも適用できる。何れの場合でも、記録媒体を収納する筐体にICを内蔵させれば対処できる。また、記録媒体に記録するデータについても、コンピュータ用のプログラム以外の各種データが適用できる。

【0062】

【発明の効果】本発明によると、記録媒体に記録されたデータの暗号化プログラムが、この記録媒体を収納する筐体に取付けられたICに記憶され、暗証番号が一致しない限りこのICから暗号化プログラムを読出すことができなく、従って記録媒体に記録されたデータの復号もできなく、記録されたデータの不正使用を防止するセキュリティ性が高い。例えば、暗証番号を知らない使用者が記録媒体に記録されたデータを別の記録媒体にコピーしても、暗号化されたままでコピーされ、コピーされたデータを復号する暗号化プログラムはコピーされず、コピーされたデータを復号することは困難で、不正使用が防止される。

【0063】この場合、IC内での暗証番号の照合で、予め定めた所定回連続して不一致を検出したとき、以後の照合で暗証番号が一致しても暗号化プログラムを出力させないブロックを行うことで、不正な使用を防止する効果がより高くなる。

【0064】また、このブロックされた状態で、暗号化プログラム読出し用の暗証番号とは別に設定された暗証番号を入力させることで、ブロックの解除を行うようにしたことで、ブロックされた状態の解除が良好にできる。

【0065】さらに、IC内のメモリに付加情報を記憶させることで、暗号化プログラムが記憶されたICが効率よく使用される。

【図面の簡単な説明】

【図1】本発明の一実施例を示す斜視図である。

【図2】一実施例の要部を示す平面図である。

【図3】図2のIII-III線に沿う断面図である。

【図4】一実施例のディスクが適用されるディスク駆動装置の構成を示す平面図である。

【図5】図4のV-V線に沿う断面図である。

【図6】一実施例の内蔵ICを示す構成図である。

【図7】一実施例の内蔵ICと接続されるホストコンピュータの一例を示す構成図である。

【図8】一実施例のディスク書込み、読出し処理を示すフローチャート図である。

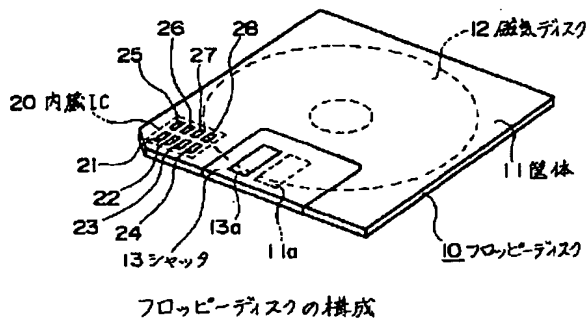
【図9】一実施例の内蔵ICとホストコンピュータとの通信状態を示す説明図である。

【符号の説明】

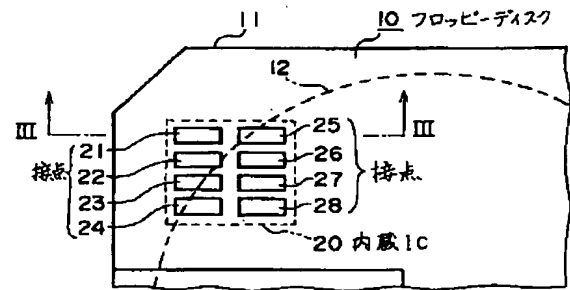
- 10 フロッピーディスク  
11 筐体  
12 磁気ディスク  
13 シャッタ  
20 内蔵IC

- 21, 22, 23, 24, 25, 26, 27, 28 接点  
30 フロッピーディスク駆動装置  
40 端子ユニット  
41, 42, 43, 44, 45, 46, 47, 48 接片  
51 中央制御装置 (CPU)  
56 ROM

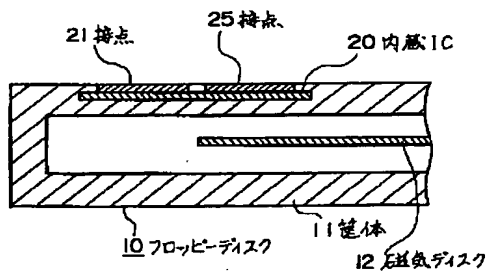
【図1】



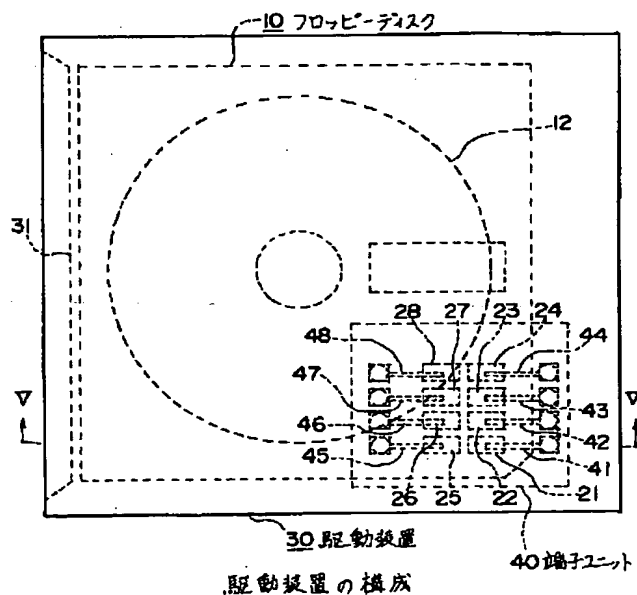
【図2】



【図3】

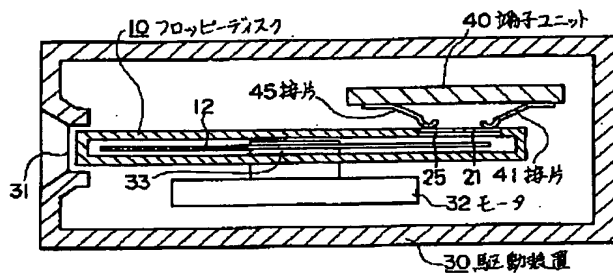


【図4】



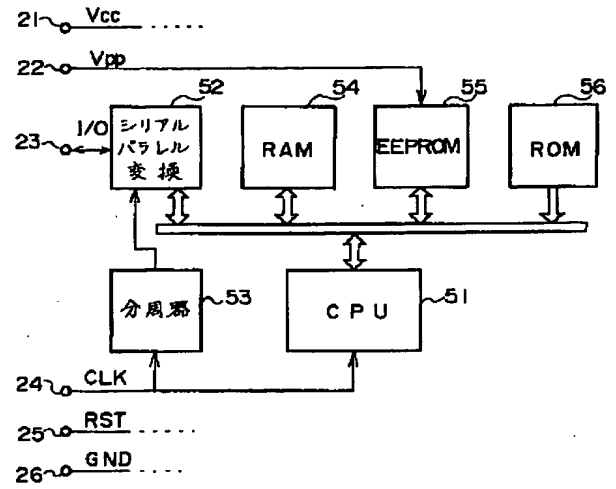


【図5】



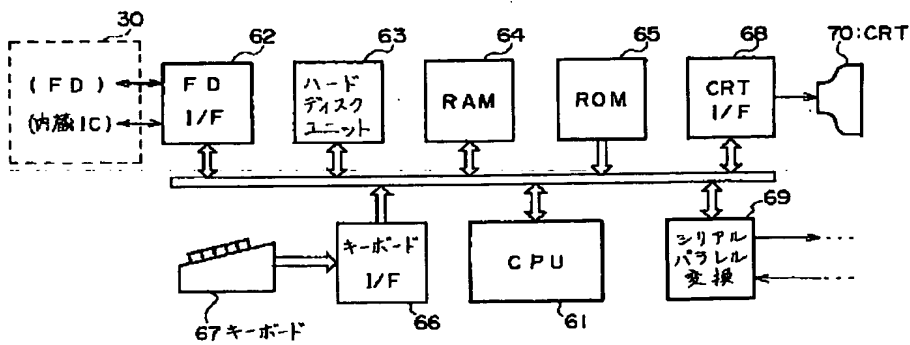
A-A 線に沿う断面図

【図6】



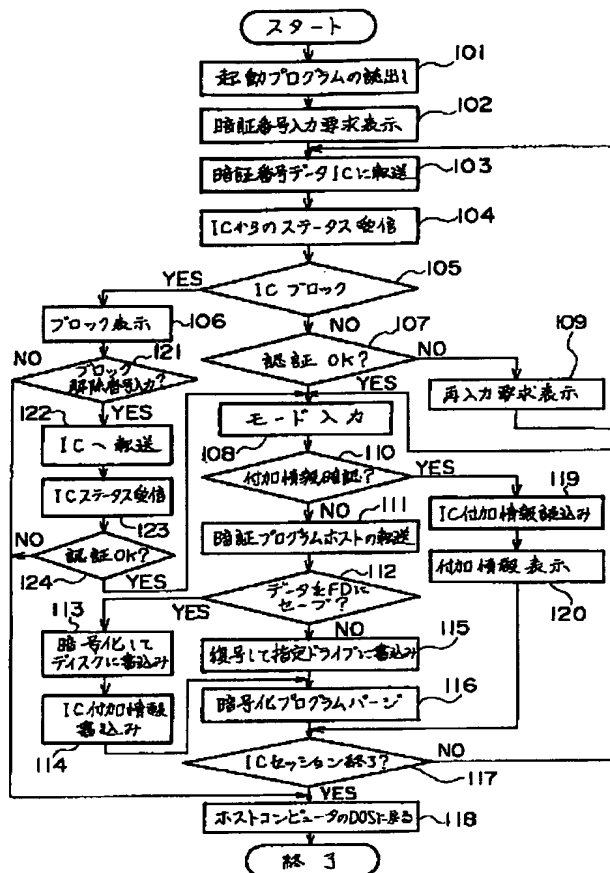
内蔵ICの構成

【図7】

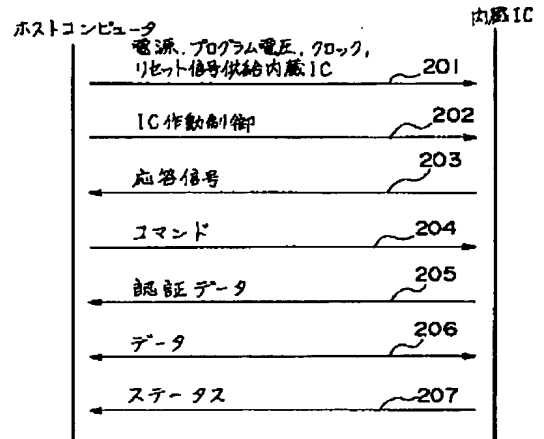


ホストコンピュータの構成

【図8】



【図9】



ホストコンピュータと内蔵ICとの通信状態